

SEALED

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF WISCONSIN

UNITED STATES OF AMERICA)
v.) Case No. 12-MJ-11
DEJAN KARABASEVIC, aka)
DAN KARABASEVIC,) COMPLAINT FOR VIOLATION OF
Defendant.) TITLE 18, UNITED STATES
) CODE, SECTIONS 1343, 1030(a)(2)(C) and
) 1030(a)(4)
)
)
)
)
)

BEFORE United States Magistrate Judge
Stephen L. Crocker

United States District Court
120 North Henry Street
Madison, Wisconsin 53703

The undersigned complainant being duly sworn states:

Count 1

Between on or about January 1, 2011, and on or about June 30, 2011, in the Western District of Wisconsin and elsewhere, the defendant, DEJAN KARABASEVIC, aka DAN KARABASEVIC, knowingly executed a scheme to defraud his employer, American Superconductor Corporation (AMSC), and to deprive AMSC of its right to KARABASEVIC's honest services.

1. It was part of the scheme that in or about February 2011, KARABASEVIC, while employed by AMSC, accepted as a bribe a six-year contract, with compensation exceeding 11 million renminbi, which equates to approximately \$1.7 million in United States dollars, to work for a Chinese manufacturer of wind energy turbines referred to herein and in the attached affidavit as Company A.

2. In or about March 2011, in the Western District of Wisconsin and elsewhere, defendant KARABASEVIC, for the purpose of executing and attempting to execute the aforementioned scheme to defraud, transmitted, and caused to be transmitted, by means of wire communication in interstate and foreign commerce, an Internet communication between an AMSC computer located in Middleton, Wisconsin, and an AMSC Windtec GmbH computer located in Klagenfurt, Austria, that transmission containing technical information, software, and source code information for AMSC products that regulate the flow of electricity from wind turbines.

3. In or about May and June 2011, in furtherance of this scheme to defraud, defendant KARABASEVIC modified the source code obtained from the AMSC computer located in Middleton, Wisconsin, and provided that information, and other proprietary information obtained from AMSC, to Company A.

(In violation of Title 18, United States Code, Section 1343).

Count 2

In or about March 2011, in the Western District of Wisconsin and elsewhere, the defendant, DEJAN KARABASEVIC, aka DAN KARABASEVIC, intentionally accessed a computer without authorization and exceeding authorized access to that computer, namely, the AMSC Middleton, Wisconsin, computer described above in Count 1, thereby obtaining information from a protected computer, namely the same computer, and the offense was committed for purposes of commercial advantage and private financial gain.

(In violation of 18 U.S.C. § 1030(a)(2)(C) and (c)(2)(B)(i)).

Count 3

In or about March 2011, in the Western District of Wisconsin and elsewhere, the defendant, DEJAN KARABASEVIC, aka DAN KARABASEVIC, knowingly and with intent to defraud accessed a protected computer without authorization and exceeded authorized access to that computer, namely, the AMSC Middleton, Wisconsin, computer described in Count 1, and by means of such conduct furthered the intended fraud described in Count 1, and in doing so obtained something of value other than the use of the computer, specifically, technical information, software, and source code information relating to AMSC products that regulate the flow of electricity from wind turbines.

(In violation of 18 U.S.C. §§ 1030(a)(4) and (c)(3)(A)).

This complaint is based on the attached affidavit of Special Agent Joshua Ben Mayers, Federal Bureau of Investigation, Madison, Wisconsin.

Joshua Ben Mayers.

JOSHUA BEN MAYERS
Federal Bureau of Investigation

Sworn to before me this 21st day of February 2011.

Stephen L. Crocker

HONORABLE STEPHEN L. CROCKER
United States Magistrate Judge

~~SEALED~~

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF WISCONSIN

UNITED STATES OF AMERICA)	
)	
v.)	
)	
DEJAN KARABASEVIC)	Case No. 12-MJ-11
aka DAN KARABASEVIC,)	
)	
Defendant.)	

AFFIDAVIT

STATE OF WISCONSIN)
) ss.
DANE COUNTY)

I, Joshua Ben Mayers, being first duly sworn on oath, depose and state as follows:

1. I have been an FBI Special Agent for 20 years. During this time, I have worked on a wide variety of Federal criminal investigations, including: wire and mail fraud; cyber crime, including child pornography and other computer-related crimes; and foreign counterintelligence, including espionage. I have had training in all of these areas and have executed Federal search warrants on email accounts, personal computers, and corporate servers.

2. I have participated in this investigation, reviewed written reports, and discussed the case with other law enforcement officers, business executives and electrical and software engineers of the victim company. I believe that the law enforcement officers are credible because they collected information pursuant to their official duties. I believe that the business executives and electrical and software engineers are credible

because their information has been corroborated by the forensic examination of electronic media discussed below, by discoveries of stolen and improperly modified software within wind turbine systems over which the victim company had no control, and by Dejan Karabasevic's confession. I have also reviewed a comprehensive report prepared by a multinational consulting corporation that acted, in this case, as private corporate fraud investigators. I believe the facts related in the comprehensive report to be reliable for the same reasons I trust the facts related to me by the representatives of the victim company. Based on this information and on my training and experience, I am providing the following information in support of this criminal complaint.

3. American Superconductor (AMSC) is a United States-domiciled company that produces software and hardware for the wind energy industry. AMSC's corporate headquarters is in Devens, Massachusetts, with additional United States offices in Middleton and New Berlin, Wisconsin. According to William Vareka, a senior software manager for AMSC, AMSC stored a certain category of source code on a server in the Middleton, Wisconsin, office in the Western District of Wisconsin at the time of the offense. In this context, source code is a set of high-level computer commands that is sent to a compiler. Vareka explained that the compiler is a computer program that transforms source code written in a programming language to binary code which can be used on a computer to perform the functions as directed by the software derived from the source code.

4. Among other things, AMSC produces equipment and software that

regulate the flow of electrical energy from wind turbines to electrical grids. Two wind turbine products that use AMSC software are the Power Module 3000 (PM3000) and the Programmable Logic Controller (PLC). These products work together using, among other programs, AMSC's Low Voltage Ride Through (LVRT) software. LVRT is designed to keep the wind turbine operational when there is a sag or dip in the electrical grid. The software that runs the PM3000 and the PLC, including the LVRT, are copyright protected and are intellectual property of AMSC. Vareka explained that the LVRT source code was created in Wisconsin and, during the spring and summer of 2011, was stored on a computer connected to the AMSC network that was located in the AMSC Middleton, Wisconsin office.

5. Vareka further advised that at some point during the summer or fall of 2010, AMSC discovered that a vulnerability in the software that ran the PLC allowed access to its source code and, as a result, Company A, a manufacturer of wind turbines domiciled in the People's Republic of China (China), was able to use the PLC without authorization. Importantly, the vulnerability did not expose the LVRT source code. Following this discovery, AMSC took measures--encryption and a 14-day limit for use of its software without a license--to protect its intellectual property. As a result of these protective measures, Company A could not use the LVRT software without contracting to do so with AMSC.

6. Daniel P. McGahn, AMSC President and Chief Executive Officer, John W. Powell, AMSC Vice President and General Counsel, and AMSC Attorney John Samia

provided the information in paragraphs 6 through 8. Dejan Karabasevic, aka Dan Karabasevic, (Karabasevic), was employed by AMSC Windtec GmbH (AMSC Windtec), in Klagenfurt, Austria. Karabasevic started with Windtec as a development engineer in 2004. In 2007, AMSC acquired Windtec which then known as AMSC Windtec. Karabasevic was eventually promoted to head of the Automation Engineering Department at AMSC Windtec. As an AMSC employee, Karabasevic certified his understanding, most recently on March 31, 2010, of AMSC's Code of Business Conduct and Ethics. That code required Karabasevic to: act in the best interests of AMSC; avoid conflicts of interest; not disclose confidential business information; protect AMSC assets; and not use AMSC assets for personal gain or the benefit of anyone else. The AMSC Information Technology Policies, acknowledged by Karabasevic on May 17, 2010, forbade use of the AMSC computer network to violate AMSC standards of ethics or to transmit proprietary information in any manner inconsistent with AMSC policies and directives. Karabasevic was not authorized to access AMSC computers to download its source code or other intellectual property to distribute to others for his own personal gain.

7. Karabasevic's job required him to travel to China to support AMSC software and hardware on behalf of AMSC. Karabasevic's work in China put him in frequent contact with employees and representatives of Company A, which in March 2011, represented nearly 80 percent of AMSC's business. On March 10, 2011, Karabasevic gave his resignation notice to his AMSC Windtec supervisor. The resignation was

accepted the following day. Pursuant to Austrian law, Karabasevic was considered "employed but on leave" until the end of June 2011. Karabasevic retained access to the AMSC Windtec office in Klagenfurt, Austria, and to the AMSC computer system.

8. In late March 2011, Company A abruptly stopped paying for shipments from AMSC. Consequently, AMSC lost substantial revenue and was forced to lay off nearly half of its work force. As AMSC's revenues fell, its market value dropped from approximately \$1.6 billion to approximately \$200 million.

9. The comprehensive report prepared by the multinational consulting company acting in this matter as private investigators (hereafter private investigators) indicates that on June 2 and June 10, 2011, AMSC China employees, while conducting field work on behalf of AMSC, discovered operational, unauthorized versions of AMSC software in use within Company A's turbines at a wind farm in China. The unauthorized versions of AMSC software contained versions of the LVRT that AMSC had not released to Company A. The AMSC China employees copied and sent the unauthorized versions to AMSC Windtec, Klagenfurt, Austria. Examination of the unauthorized versions by AMSC employees showed that the software had been modified to include removal of the encryption and the 14-day unlicensed use limitation. The AMSC employees concluded that the changes could not have been made without access to the LVRT source code. As noted above, the development folder for the LVRT source code was only stored at the AMSC office in Middleton, Wisconsin. AMSC officials suspected that Karabasevic had provided the unauthorized source code to Company A.

10. Emails found within Karabasevic's computers obtained from his Beijing and Klagenfurt, Austria, apartments--the searches of which are described below--as well as documents found in Karabasevic's Beijing apartment, showed that between approximately September 2010 and February 2011, Karabasevic negotiated an employment contract with Company A. Karabasevic and Company A agreed to a six-year contact beginning in May 2011, with Karabasevic's total compensation exceeding 11 million renminbi, which equates to approximately \$1.7 million U.S. dollars.

11. Karabasevic was confronted by AMSC Windtec personnel on June 30, 2011. Karabasevic gave a statement on that day and then provided a signed statement on July 28, 2011. I have reviewed a translated copy of Karabasevic's statement. In his signed statement, Karabasevic admitted to downloading the PM3000 source code (which included the LVRT source code) from the AMSC computer network. Karabasevic admitted that he downloaded the entire PM3000 folder through the AMSC network to his office at AMSC Windtec, Klagenfurt, Austria, to his AMSC Windtec laptop, then to an external drive, and then to another laptop. As noted above, the development folder was stored exclusively at the AMSC office in Middleton, Wisconsin. Karabasevic further admitted to downloading other proprietary AMSC information from the computers at AMSC Windtec, Klagenfurt, Austria. Karabasevic admitted that he provided improperly-taken AMSC software to Company A employees, and he then traveled to China where he adapted AMSC software, including the software containing the LVRT functionality, for use in Company A's wind turbines. Karabasevic admitted that he knew

what he was doing was wrong. Karabasevic further admitted that he had negotiated an employment contract with Company A.

12. On July 9, 2011, Karabasevic gave written permission, in the presence of a representative of DBJ, an Austrian law firm, to search the Beijing apartment that Company A had arranged for him. On the same day, private detectives searched Karabasevic's Beijing apartment, finding two notebook computers, an external hard drive, and documents. Included within the documents were employment contracts between Karabasevic and Company A. The next day, July 10, 2011, at the Vienna, Austria airport, an AMSC China employee turned over the evidence obtained from Karabasevic's Beijing apartment to a representative of the private investigative firm. Subsequently, the Beijing evidence was turned over to Austrian law enforcement authorities through DBJ, the Austrian law firm. Around the same period, Austrian law enforcement officers secured computers and other electronic storage media from Karabasevic's Klagenfurt, Austria apartment. Forensic copies of the computers and electronic storage media obtained from Karabasevic's Beijing and Klagenfurt apartments were analyzed by forensic analysts working with the private investigative firm referenced above. The forensic examination of the computers and electronic storage media found in Karabasevic's Beijing and Klagenfurt apartments showed that he had stored, possessed, and manipulated AMSC proprietary data--downloaded from AMSC Windtec in Klagenfurt, Austria, and AMSC in Middleton, Wisconsin--on the computers and electronic storage media. In particular, AMSC copyrighted and proprietary technical

information, software, and source code information--to include the entire development folder containing multiple versions of the LVRT source code--that had been downloaded from the AMSC Middleton, Wisconsin, computer were found on a notebook computer found in Karabasevic's Beijing apartment. The analysis further showed, consistent with Karabasevic's confession described herein, that the information electronically transmitted from AMSC Middleton to AMSC Windtec, Klagenfurt, Austria, had been adapted for use with equipment associated with Company A's wind turbines.

Dated this 21 day of February 2012.

Joshua Ben Mayers.
SPECIAL AGENT JOSHUA BEN MAYERS
Federal Bureau of Investigation Agency

Sworn to before me this 21st day of February 2012.

Stephen L. Crocker
STEPHEN L. CROCKER
United States Magistrate Judge